



# Analysis & Correlation of Mac Logs

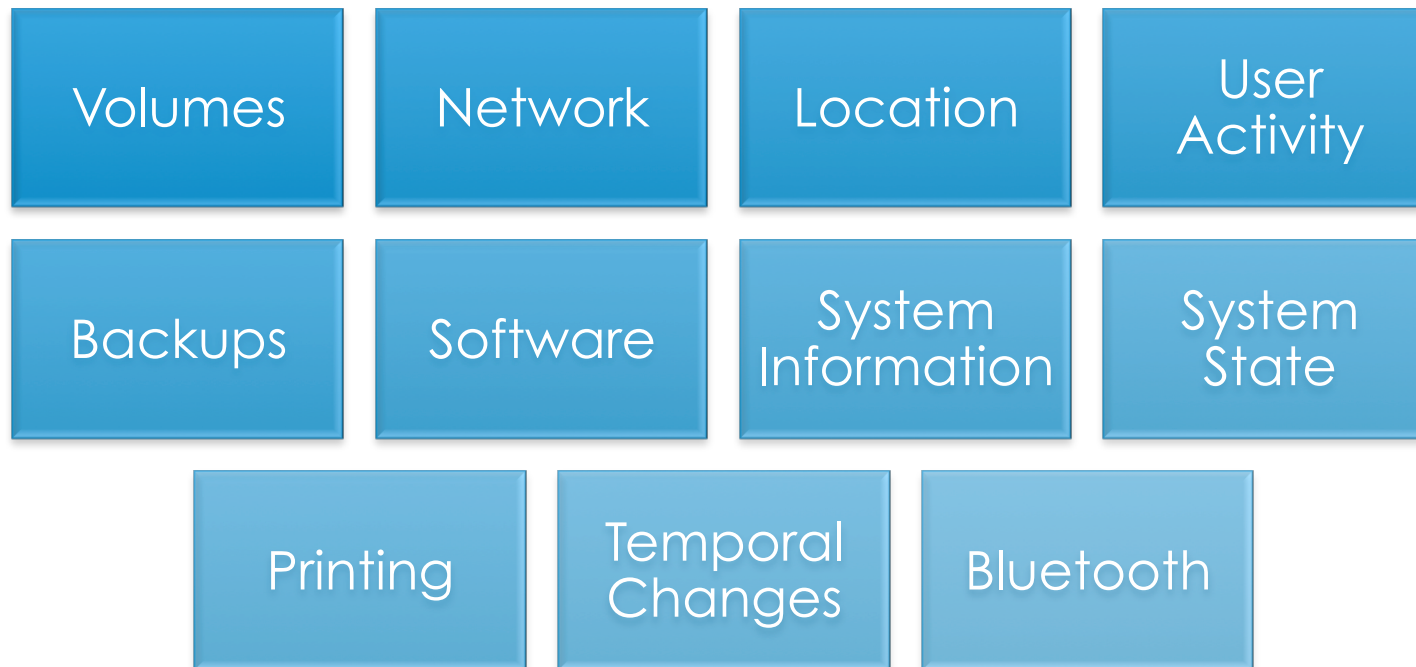
Sarah Edwards  
@iamevltwin  
oompa@csh.rit.edu

---

# About Me

- Senior Digital Forensics Analyst
- Crucial Security (Harris Corporation)
- Northern Virginia
- Federal Law Enforcement
- Intrusion Analysis
- Counter-Intelligence, Counter-Terrorism, Criminal Cases
- Mac Nerd at heart.
- Blog: [crucialsecurityblog.harris.com](http://crucialsecurityblog.harris.com)

# Why?



# Log Basics



# General Location

## System Logs

- /var/log
- /Library/Logs

## User Logs

- ~/Library/Logs

## Application Specific

- /Library/Application Support/<app>
- /Applications/

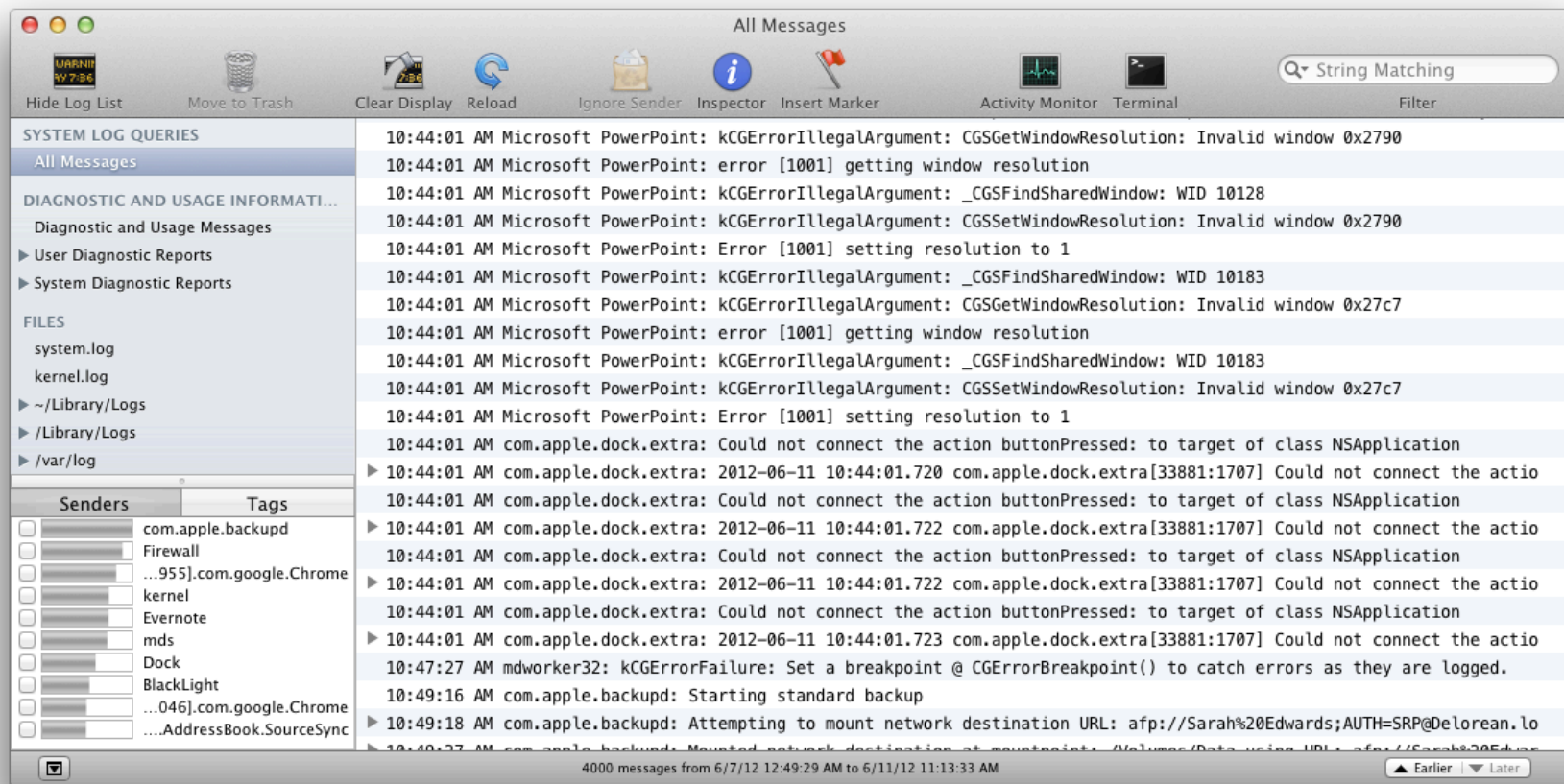
# OS X Log Basics

- Tends to use Standard Unix Log Format
  - MMM DD HH:MM:SS Host Service: Message
- Most are in plaintext
- BZip2 Compression
  - Used for archival after log turnover

```
Apr 18 22:44:02 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:02 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:04 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:04 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:10 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:10 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:22 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:22 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:46 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 22:44:46 byte Firewall[89]: Stealth Mode connection attempt
Apr 18 23:01:12 byte Firewall[89]: Stealth Mode connection attempt
```

```
appfirewall.log
appfirewall.log.0.bz2
appfirewall.log.1.bz2
appfirewall.log.2.bz2
appfirewall.log.3.bz2
appfirewall.log.4.bz2
appfirewall.log.5.bz2
```

# Console.app



# Console.app: Message Inspector

```
4/6/12 4:45:20 PM login: USER_PROCESS: 304 ttys004
4/6/12 4:45:21 PM login: USER_PROCESS: 308 ttys005
4/28/12 3:31:05 PM login: DEAD_PROCESS: 278 ttys000
4/28/12 3:31:05 PM login: DEAD_PROCESS: 300 ttys003
4/28/12 3:31:05 PM login: DEAD_PROCESS: 292 ttys001
4/28/12 3:31:05 PM login: DEAD_PROCESS: 296 ttys002
4/28/12 3:31:06 PM login: DEAD_PROCESS: 304 ttys004
4/28/12 3:31:06 PM login: DEAD_PROCESS: 308 ttys005
4/28/12 5:36:50 PM login: USER_PROCESS: 96459 ttys000
4/28/12 5:36:50 PM login: USER_PROCESS: 96460 ttys001
4/28/12 5:36:51 PM login: USER_PROCESS: 96467 ttys002
4/28/12 5:36:51 PM login: USER_PROCESS: 96471 ttys003
4/28/12 5:36:51 PM login: USER_PROCESS: 96472 ttys004
4/28/12 5:36:51 PM login: USER_PROCESS: 96479 ttys005
5/15/12 10:44:23 AM login: DEAD_PROCESS: 96459 ttys000
5/15/12 10:44:23 AM login: DEAD_PROCESS: 96460 ttys001
5/15/12 10:44:24 AM login: DEAD_PROCESS: 96467 ttys002
5/15/12 10:44:25 AM login: DEAD_PROCESS: 96471 ttys003
5/15/12 10:44:27 AM login: DEAD_PROCESS: 96479 ttys005
5/15/12 10:44:59 AM login: USER_PROCESS: 35204 ttys000
5/15/12 7:44:24 PM sshd: USER_PROCESS: 39491 ttys001
5/15/12 8:08:56 PM sshd: DEAD_PROCESS: 39491 ttys001
5/20/12 12:43:58 PM sshd: USER_PROCESS: 49332 ttys001
5/20/12 12:48:19 PM sshd: DEAD_PROCESS: 49332 ttys001
```

| Message Inspector |                             |
|-------------------|-----------------------------|
| Key               | Value                       |
| ASLExpireTime     | 1368747864                  |
| ASLMessageID      | 3546564                     |
| Facility          | com.apple.system.lastlog    |
| GID               | 0                           |
| Host              | byte                        |
| Level             | 5                           |
| PID               | 39488                       |
| ReadGID           | 80                          |
| Sender            | sshd                        |
| Time              | 1337125464                  |
| TimeNanoSec       | 436116000                   |
| UID               | 0                           |
| ut_host           | bit                         |
| ut_id             | s001                        |
| ut_line           | ttys001                     |
| ut_pid            | 39491                       |
| ut_tv.tv_sec      | 1337125464                  |
| ut_tv.tv_usec     | 420174                      |
| ut_type           | 7                           |
| ut_user           | oompa                       |
| Message           | USER_PROCESS: 39491 ttys001 |

# Log Friendly Software

- View the BZip2 compressed files easily:
  - Console.app
  - FTK Imager
  - BlackBag Blacklight
  - X-Ways
  - TextWrangler
- Not so friendly:
  - Encase 6
    - Must extract the files and decompress.

# BZip2 Decompression

- Use `bzcat` on OS X
  - (oldest -> newest)
  - `system.log.7.bz2` -> `system.log.0.bz2`

1. `bzcat system.log.7.bz2 system.log.6.bz2 system.log.5.bz2 system.log.4.bz2 system.log.3.bz2 system.log.2.bz2 system.log.1.bz2 system.log.0.bz2 >> system_all.log`
2. `cat system.log >> system_all.log`

# Log Recovery

- Logs get “removed” or “turned over”
- GREP or keyword search for specific date/  
log formats.
  - “May 18 23:17:15”
  - “Thu May 31 19:35:35 EDT 2012”
  - “ASL DB”
  - “launchctl::Audit startup”
  - “BZh91AY&SY”

# Apple System Log



# Apple System Log

- Location: /private/var/log/asl/ (>10.5.6)
- syslog “replacement”
- View using Console.app or `syslog` command
- Filename Format: YYYY.MM.DD.[UID].[GID].asl
- Binary Format

```
-rw-----+ 1 root  wheel  93522 May 22 23:45 2012.05.22.G80.asl
-rw-----+ 1 root  wheel   8696 May 22 23:45 2012.05.22.U0.G80.asl
-rw-----+ 1 root  wheel  24612 May 22 23:45 2012.05.22.U501.asl
-rw-----+ 1 root  wheel   3720 May 22 22:45 2012.05.22.U89.asl
-rw-----+ 1 root  wheel  87101 May 23 23:45 2012.05.23.G80.asl
-rw-----+ 1 root  wheel   9245 May 23 23:45 2012.05.23.U0.G80.asl
-rw----- 1 root  wheel    864 May 23 21:57 2012.05.23.U0.asl
-rw-----+ 1 root  wheel  18556 May 23 23:35 2012.05.23.U501.asl
-rw-----+ 1 root  wheel   5680 May 23 23:45 2012.05.23.U89.asl
-rw-----+ 1 root  wheel  92582 May 24 23:45 2012.05.24.G80.asl
-rw-----+ 1 root  wheel   9122 May 24 23:45 2012.05.24.U0.G80.asl
-rw-----+ 1 root  wheel  17707 May 24 23:28 2012.05.24.U501.asl
-rw-----+ 1 root  wheel   5680 May 24 23:45 2012.05.24.U89.asl
-rw-----+ 1 root  wheel  92416 May 25 23:45 2012.05.25.G80.asl
```

# Legacy ASL

## 10.4

- /var/log/asl.log
- Plaintext

## 10.5 – 10.5.6

- /var/log/asl.db
- Binary Format
- “ASL DB” File Header
- Use `syslog -f` to view

# syslog Command

## Output Format (-F)

bsd

std

raw

xml

## Time Format (-T)

sec

local

utc

## File or Directory

-f

-d

```
sh-3.2# syslog -d asl/ | more
Mar 12 17:15:01 byte login[63585] <Notice>: USER_PROCESS: 63585 ttys003
Mar 15 01:41:32 byte login[48848] <Notice>: USER_PROCESS: 48848 ttys004
Mar 15 01:44:22 byte login[48905] <Notice>: USER_PROCESS: 48905 ttys005
Mar 15 01:52:19 byte login[48848] <Notice>: DEAD_PROCESS: 48848 ttys004
Mar 15 01:52:19 byte login[48905] <Notice>: DEAD_PROCESS: 48905 ttys005
Mar 15 01:52:21 byte login[48960] <Notice>: USER_PROCESS: 48960 ttys004
Mar 15 01:53:16 byte login[48960] <Notice>: DEAD_PROCESS: 48960 ttys004
Mar 15 01:53:18 byte login[50861] <Notice>: USER_PROCESS: 50861 ttys004
Mar 15 01:53:52 byte login[50861] <Notice>: DEAD_PROCESS: 50861 ttys004
Mar 15 01:53:53 byte login[52753] <Notice>: USER_PROCESS: 52753 ttys004
Mar 15 01:54:19 byte login[53625] <Notice>: USER_PROCESS: 53625 ttys005
```



# syslog -T utc -F raw -d /asl

- [ASLMessageID 3555356]
- [Time 2012.05.28 19:39:32 UTC]
- [TimeNanoSec 887175000]
- [Level 5]
- [PID 908]
- [UID 0]
- [GID 20]
- [ReadGID 80]
- [Host byte]
- [Sender login]
- [Facility com.apple.system.utmpx]
- [Message DEAD\_PROCESS: 908 ttys002]
- [ut\_user oompa]
- [ut\_id s002]
- [ut\_line ttys002]
- [ut\_pid 908]
- [ut\_type 8]
- [ut\_tv.tv\_sec 1338233972]
- [ut\_tv.tv\_usec 886961]
- [ASLExpireTime 1369856372]

# Audit Logs

# Audit Logs

- Location: /private/var/audit/
- BSM Audit Logs
- StartTime.EndTime
- YYYYMMDDHHMMSS.YYYYMMDDHHMMSS
- Binary Format

```
drwx-----  8 root  wheel    272 May 28 15:22 .
drwxr-xr-x  29 root  wheel    986 May  9 21:39 ..
-r--r-----  1 root  wheel  48987 May 10 00:46 20120509232853.20120510044637
-r--r-----  1 root  wheel  57158 May 12 11:31 20120510204054.20120512153135
-r--r-----  1 root  wheel  92166 May 27 20:02 20120512153220.20120528000216
-r--r-----  1 root  wheel  20805 May 28 15:20 20120528000250.20120528192006
-r--r-----  1 root  wheel   4619 May 28 21:07 20120528192235.not_terminated
lrwxr-xr-x   1 root  wheel    40 May 28 15:22 current -> /var/audit/20120528192235.not_terminated
```

# praudit -xn /var/audit/\*

- su Example:

```
<record version="11" event="user authentication" modifier="0" time="Mon May 28
21:12:51 2012" msec=" + 41 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20" pid="552"
sid="100004" tid="552 0.0.0.0" />
<text>Verify password for record type Users &apos;root&apos; node &apos;/Local/
Default&apos;;</text>
<return errval="success" retval="0" />
</record>

<record version="11" event="user authentication" modifier="0" time="Mon May 28
21:12:55 2012" msec=" + 449 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20" pid="554"
sid="100004" tid="554 0.0.0.0" />
<text>Verify password for record type Users &apos;root&apos; node &apos;/Local/
Default&apos;;</text>
<return errval="failure: Unknown error: 255" retval="5000" />
</record>
```

# Audit Log Records

- Each record is made up of “tokens”:
  - Header
  - Subject
  - Text
  - Return
  - Trailer

```
<record version="11" event="user authentication"
modifier="0" time="Mon May 28 21:12:51 2012" msec=" +
41 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501"
rgid="20" pid="552" sid="100004" tid="552 0.0.0.0" />
<text>Verify password for record type Users
&apos;root&apos; node &apos;/Local/Default&apos;</
text>
<return errval="success" retval="0" />
</record>
```



# Audit Log Record - Tokens

- Variable number of tokens
- Each is described in the `audit.log` man page.

## Subject Token

The ``subject'' token contains information on the subject performing the operation described by an audit record, and includes similar information to that found in the ``process'' and ``expanded process'' tokens. However, those tokens are used where the process being described is the target of the operation, not the authorizing party. A ``subject'' token can be created using `au_to_subject32(3)` and `au_to_subject64(3)`.

| Field                    | Bytes     | Description                   |
|--------------------------|-----------|-------------------------------|
| Token ID                 | 1 byte    | Token ID                      |
| Audit ID                 | 4 bytes   | Audit user ID                 |
| Effective User ID        | 4 bytes   | Effective user ID             |
| Effective Group ID       | 4 bytes   | Effective group ID            |
| Real User ID             | 4 bytes   | Real user ID                  |
| Real Group ID            | 4 bytes   | Real group ID                 |
| Process ID               | 4 bytes   | Process ID                    |
| Session ID               | 4 bytes   | Audit session ID              |
| Terminal Port ID         | 4/8 bytes | Terminal port ID (32/64-bits) |
| Terminal Machine Address | 4 bytes   | IP address of machine         |

# Volumes

# system.log & daily.log

## Search “/Volumes/”

```
May 19 08:58:23 bit fsevents[20]: log dir: /Volumes/Time Machine Backups/.fsevents getting new uuid: 5420A642-DE8C-4B90-B2B4-B948288F5E3F
May 19 16:52:30 bit fsevents[20]: log dir: /Volumes/NO NAME/.fsevents getting new uuid: DD64986D-F58C-407B-901B-5BD27104F062
May 23 20:10:35 bit fsevents[20]: log dir: /Volumes/NO NAME/.fsevents getting new uuid: 0D8CB03B-0691-4381-ACEF-8F7F421D12DF
May 26 14:01:03 bit fsevents[20]: log dir: /Volumes/WDPassport/.fsevents getting new uuid: CDCE4339-A254-4925-A909-97B4553BDAC1
May 26 15:40:38 bit fsevents[20]: log dir: /Volumes/WDPassport/.fsevents getting new uuid: D4FFFB2-16A8-4CB3-88DE-327CDE1551EC
```

Fri May 11 17:12:29 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

Disk status:

| Filesystem                        | Size  | Used  | Avail | Capacity | Mounted on             |
|-----------------------------------|-------|-------|-------|----------|------------------------|
| /dev/disk0s2                      | 698Gi | 22Gi  | 675Gi | 4%       | /                      |
| localhost:/35wJAmjuh-MSBDh6mJulon | 698Gi | 698Gi | 0Bi   | 100%     | /Volumes/MobileBackups |
| /dev/disk6s2                      | 107Mi | 107Mi | 0Bi   | 100%     | /Volumes/Google Chrome |

# kernel.log

## Search “USBMSC”

- Serial Number, Vendor ID, Product ID, Version

```
Apr 25 12:27:11 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:32:31 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:47:29 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:49:43 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 12:52:46 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 25 12:53:37 Pro kernel[0]: USBMSC Identifier (non-unique): ABCDEF0123456789 0xe90 0x5 0x0
Apr 25 13:04:21 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 25 13:04:29 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 26 12:36:05 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
Apr 27 09:02:59 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
Apr 30 09:07:14 Pro kernel[0]: USBMSC Identifier (non-unique): FBF1011220504638 0x90c 0x1000 0x1100
May 3 05:43:05 Pro kernel[0]: USBMSC Identifier (non-unique): 58A8120830AC8C5C 0x1e1d 0x1101 0x100
May 3 06:24:05 Pro kernel[0]: USBMSC Identifier (non-unique): SWOC22905731 0x1199 0xffff 0x323
May 24 11:22:43 Pro kernel[0]: USBMSC Identifier (non-unique): 000000009833 0x5ac 0x8403 0x9833
May 24 11:53:25 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 25 12:48:38 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 30 06:50:01 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
May 31 13:10:09 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
Jun 1 07:16:03 Pro kernel[0]: USBMSC Identifier (non-unique): 0911201415f7f3 0x1e1d 0x165 0x100
```

# USBMSC - kernel.log

## System Information

```
Jun  3 11:11:53 bit kernel[0]: USBMSC Identifier  
(non-unique): FBF1011220504638 0x90c 0x1000 0x1100
```

### Flash Disk:

|                         |                                        |
|-------------------------|----------------------------------------|
| Capacity:               | 8.02 GB (8,019,509,248 bytes)          |
| Removable Media:        | Yes                                    |
| Detachable Drive:       | Yes                                    |
| BSD Name:               | disk2                                  |
| Product ID:             | 0x1000                                 |
| Vendor ID:              | 0x090c (Silicon Motion, Inc. - Taiwan) |
| Version:                | 11.00                                  |
| Serial Number:          | FBF1011220504638                       |
| Speed:                  | Up to 480 Mb/sec                       |
| Manufacturer:           | USB                                    |
| Location ID:            | 0xfd130000 / 5                         |
| Current Available (mA): | 500                                    |
| Current Required (mA):  | 500                                    |
| Partition Map Type:     | MBR (Master Boot Record)               |
| S.M.A.R.T. status:      | Not Supported                          |

### Volumes:

#### BLACKBAG:

|              |                               |
|--------------|-------------------------------|
| Capacity:    | 8.02 GB (8,019,476,992 bytes) |
| Available:   | 7.87 GB (7,868,444,672 bytes) |
| Writable:    | Yes                           |
| File System: | MS-DOS FAT32                  |
| BSD Name:    | disk2s1                       |
| Mount Point: | /Volumes/BLACKBAG             |
| Content:     | DOS_FAT_32                    |

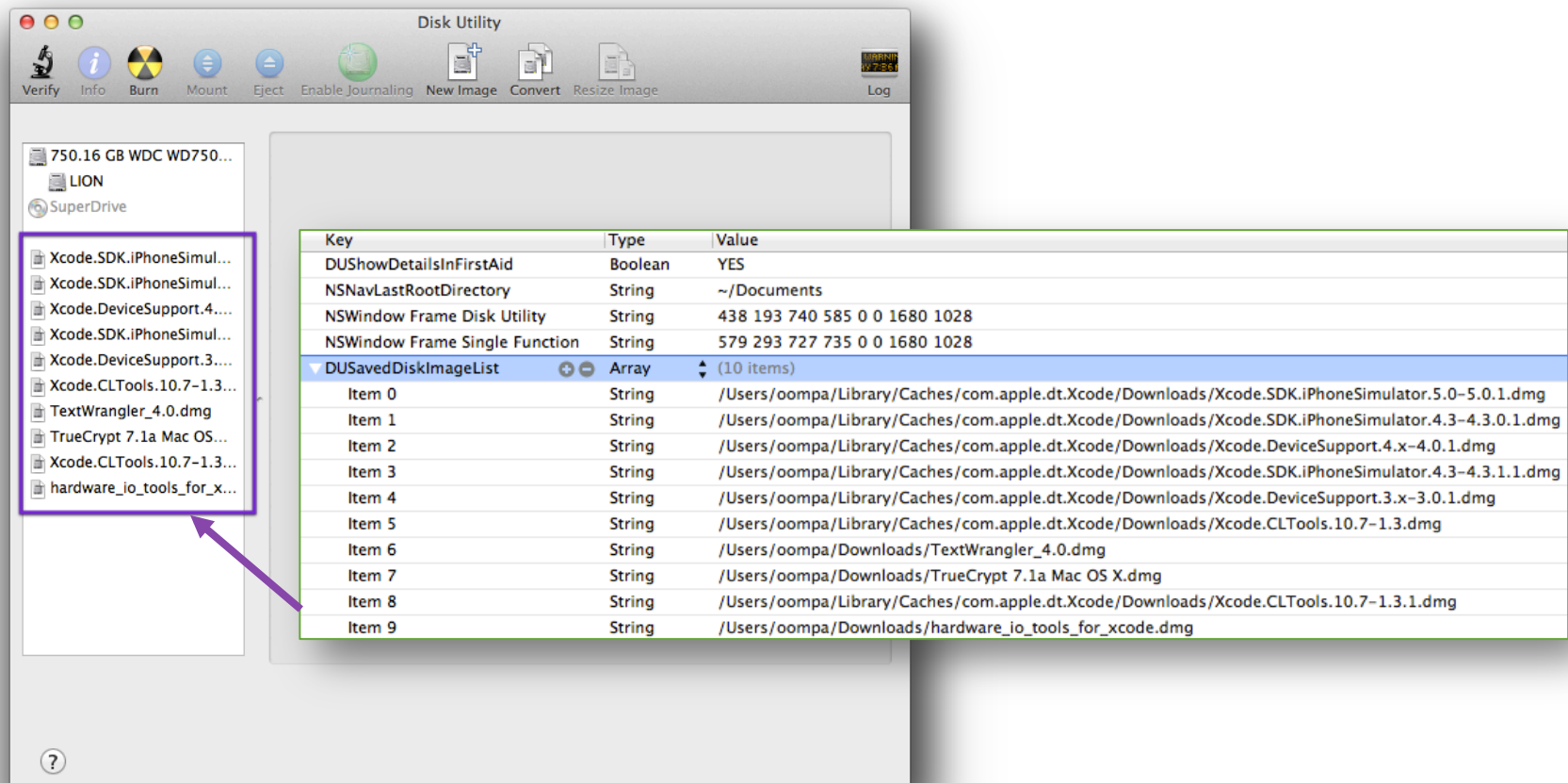
# ~/Library/Preferences/ com.apple.finder.plist

- FXDesktopVolumePositions
- FXRecentFolders (10 most recent)

|                   |            |                    |
|-------------------|------------|--------------------|
| ▼ FXRecentFolders | Array      | (10 items)         |
| ▼ Item 0          | Diction... | (2 items)          |
| file-bookmark     | Data       | <626f6f6b ac030000 |
| name              | String     | STUFF              |
| ▼ Item 1          | Diction... | (2 items)          |
| file-bookmark     | Data       | <626f6f6b 3c030000 |
| name              | String     | TechnoSecurity2012 |
| ▼ Item 2          | Diction... | (2 items)          |
| file-bookmark     | Data       | <626f6f6b 8c020000 |
| name              | String     | oompa              |
| ▼ Item 3          | Diction... | (2 items)          |
| file-bookmark     | Data       | <626f6f6b c0020000 |
| name              | String     | Dropbox            |

|                                     |
|-------------------------------------|
| Key                                 |
| ▼ FXDesktopVolumePositions          |
| ▶ STUFF_-0x1.d27e44p+29             |
| ▶ VMware Fusion_0x1.3f5f0e2p+28     |
| ▶ WDPassport_-0x1.d27e44p+29        |
| ▶ DATA_0x1.3db4fc2p+28              |
| ▶ OmniOutliner_0x1.25dcb04p+27      |
| ▶ Sample Docs_0x1.eefdap+26         |
| ▶ NO NAME_-0x1.3c0752p+29           |
| ▶ OmniOutliner Pro_0x1.25dcad2p+27  |
| ▶ Time Machine Backups_0x1.438f33dp |

# ~/Library/Preferences/ com.apple.DiskUtility.plist



~/Library/Preferences/  
com.apple.sidebarlists.plist

| Key                    | Type       | Value       |
|------------------------|------------|-------------|
| ▼ favorites            | Diction... | (7 items)   |
| ▶ CustomListProperties | Diction... | (2 items)   |
| ShowRemovable          | Boolean    | YES         |
| ShowHardDisks          | Boolean    | YES         |
| ShowEjectables         | Boolean    | YES         |
| ▶ VolumesList          | Array      | (57 items)  |
| ShowServers            | Boolean    | YES         |
| Controller             | String     | VolumesList |
| ▶ savedsearches        | Diction... | (2 items)   |
| ▼ systemitems          | Diction... | (7 items)   |
| ▶ CustomListProperties | Diction... | (1 item)    |
| ShowRemovable          | Boolean    | YES         |
| ShowHardDisks          | Boolean    | YES         |
| ShowEjectables         | Boolean    | YES         |
| ▶ VolumesList          | Array      | (42 items)  |
| ShowServers            | Boolean    | YES         |
| Controller             | String     | VolumesList |

|               |            |                                               |
|---------------|------------|-----------------------------------------------|
| ▼ VolumesList | Array      | (42 items)                                    |
| ▶ Item 0      | Diction... | (4 items)                                     |
| ▶ Item 1      | Diction... | (5 items)                                     |
| ▶ Item 2      | Diction... | (3 items)                                     |
| ▶ Item 3      | Diction... | (4 items)                                     |
| ▶ Item 4      | Diction... | (5 items)                                     |
| ▶ Item 5      | Diction... | (4 items)                                     |
| ▼ Item 6      | Diction... | (3 items)                                     |
| Alias         | Data       | <00000000 00b40003 00010000 cbc9d31f 0000482b |
| Name          | String     | Dropbox Installer                             |
| EntryType     | Number     | 1027                                          |
| ▼ Item 7      | Diction... | (3 items)                                     |
| Alias         | Data       | <00000000 00a00003 00010000 cbc0e521 0000482b |
| Name          | String     | Google Chrome                                 |
| EntryType     | Number     | 1027                                          |
| ▼ Item 8      | Diction... | (3 items)                                     |
| Alias         | Data       | <00000000 00740003 00010000 ca50c8c2 0000482b |
| Name          | String     | DATA                                          |
| EntryType     | Number     | 517                                           |



# com.apple.sidebarlists.plist

## Volume EntryType

261 – HDD (Boot HDD)

16

- Network HDD
- iDisk
- “Computer”

1027

- Disk Image
- DVD

1029 - Unknown

515

- USB Flash
- Time Machine

517 – USB HDD

|               |            |                                               |
|---------------|------------|-----------------------------------------------|
| ▼ VolumesList | Array      | (42 items)                                    |
| ▶ Item 0      | Diction... | (4 items)                                     |
| ▶ Item 1      | Diction... | (5 items)                                     |
| ▶ Item 2      | Diction... | (3 items)                                     |
| ▶ Item 3      | Diction... | (4 items)                                     |
| ▶ Item 4      | Diction... | (5 items)                                     |
| ▶ Item 5      | Diction... | (4 items)                                     |
| ▼ Item 6      | Diction... | (3 items)                                     |
| Alias         | Data       | <00000000 00b40003 00010000 cbc9d31f 0000482b |
| Name          | String     | Dropbox Installer                             |
| EntryType     | Number     | 1027                                          |
| ▼ Item 7      | Diction... | (3 items)                                     |
| Alias         | Data       | <00000000 00a00003 00010000 cbc0e521 0000482b |
| Name          | String     | Google Chrome                                 |
| EntryType     | Number     | 1027                                          |
| ▼ Item 8      | Diction... | (3 items)                                     |
| Alias         | Data       | <00000000 00740003 00010000 ca50c8c2 0000482b |
| Name          | String     | DATA                                          |
| EntryType     | Number     | 517                                           |

\_\_\_\_\_

BDxF - ExFAT

BDIS – FAT32

BDcu –UDF (DVD)

NTcu - Unknown

H<sup>+</sup> - HFS

|           |            |                                               |
|-----------|------------|-----------------------------------------------|
| ▼ Item 38 | Diction... | (3 items)                                     |
| Alias     | Data       | <00000000 008c0003 00010000 cbe15767 0000482b |
| Name      | String     | Wireshark                                     |
| EntryType | Number     | 1027                                          |

|     |             |             |             |             |             |       |                      |
|-----|-------------|-------------|-------------|-------------|-------------|-------|----------------------|
| 000 | 00 00 00 00 | 00 8C 00 03 | 00 01 00 00 | CB E1 57 67 | 00 00 48 2B | 00 00 | \\\\\\WireShark\\    |
| 022 | 00 05 00 00 | 00 01 00 00 | 00 02 00 00 | CB E1 57 67 | 00 00 00 00 | 0D 02 | \\\\\\WireShark\\    |
| 044 | FF FE 00 00 | 00 00 00 00 | 00 00 FF FF | FF FF 00 01 | 00 00 00 0E | 00 14 | \\\\\\WireShark\\    |
| 066 | 00 09 00 57 | 00 69 00 72 | 00 65 00 73 | 00 68 00 61 | 00 72 00 6B | 00 0F | \\\\\\WireShark\\    |
| 088 | 00 14 00 09 | 00 57 00 69 | 00 72 00 65 | 00 73 00 68 | 00 61 00 72 | 00 6B | \\\\\\WireShark\\    |
| 110 | 00 12 00 00 | 00 13 00 12 | 2F 56 6F 6C | 75 6D 65 73 | 2F 57 69 72 | 65 73 | \\\\\\Volumes\\WireS |
| 132 | 68 61 72 6B | FF FF 00 00 |             |             |             |       | hark \\              |

# Volume Alias Data Dates & Mount Point

- File Creation Time (HFS Date)
- May or may not be present
  - Only seen on H+ formatted disks
  - DMG
  - USB

|     |             |             |             |             |             |       |       |                    |
|-----|-------------|-------------|-------------|-------------|-------------|-------|-------|--------------------|
| 000 | 00 00 00 00 | 00 8C 00 03 | 00 01 00 00 | CB E1 57 67 | 00 00 48 2B | 00 00 | ~~~~~ | Wg~H+~             |
| 022 | 00 05 00 00 | 00 01 00 00 | 00 02 00 00 | CB E1 57 67 | 00 00 00 00 | 0D 02 | ~~~~~ | Wg~\$~             |
| 044 | FF FE 00 00 | 00 00 00 00 | 00 00 FF FF | FF FF 00 01 | 00 00 00 0E | 00 14 | ~~~~~ |                    |
| 066 | 00 09 00 57 | 00 69 00 72 | 00 65 00 73 | 00 68 00 61 | 00 72 00 6B | 00 0F | ~~~~~ | W~i~r~e~s~h~a~r~k~ |
| 088 | 00 14 00 09 | 00 57 00 69 | 00 72 00 65 | 00 73 00 68 | 00 61 00 72 | 00 6B | ~~~~~ | W~i~r~e~s~h~a~r~k~ |
| 110 | 00 12 00 00 | 00 13 00 12 | 2F 56 6F 6C | 75 6D 65 73 | 2F 57 69 72 | 65 73 | ~~~~~ | /Volumes/Wires     |
| 132 | 68 61 72 6B | FF FF 00 00 |             |             |             |       | ~~~~~ | hark ~             |

# Network Information

# Network Changes system.log

```
Jun 12 13:07:11 bit configd[16]: network configuration changed.  
Jun 12 13:07:11 bit configd[16]: setting hostname to "bit.local"  
Jun 12 13:07:11 bit configd[16]: network configuration changed.  
Jun 12 13:07:24 bit ntpd[50]: bind(25) AF_INET6 fe80::9227:e4ff:fef8:e65f%5#123  
flags 0x11 failed: Can't assign requested address  
Jun 12 13:07:24 bit airportd[3218]: _doAutoJoin: Already associated to "PANERA".  
Bailing on auto-join.  
Jun 12 13:07:28 bit configd[16]: network configuration changed.
```

# system.log

## Search "airportd"

```
Jun 12 10:17:24 bit airportd[36]: _doAutoJoin: Already associated to "veyron". Bailing on auto-join.
Jun 12 11:43:17 bit airportd[3105]: _doAutoJoin: Already associated to "veyron". Bailing on auto-join.
Jun 12 13:07:24 bit airportd[3218]: _doAutoJoin: Already associated to "PANERA". Bailing on auto-join.
Jun 12 13:07:29 bit airportd[3218]: _doAutoJoin: Already associated to "PANERA". Bailing on auto-join.
Jun 12 14:51:42 bit airportd[3756]: _processSystemPSKAssoc: No password for network <CWNetwork: 0x7f8083c189b0> [ssid=L.A. Boxing Customer WIFI, bssid=00:21:29:d5:20:12, security=WPA/WPA2 Personal, rssi=-92, channel=<CWChannel: 0x7f8085106d90> [channelNumber=6(2GHz), channelWidth={20MHz}], ibss=0] in the system keychain
Jun 12 16:49:03 bit airportd[3769]: _doAutoJoin: Already associated to "veyron". Bailing on auto-join.
```

/Library/Preferences/SystemConfiguration/  
com.apple.airport.preferences.plist

| Key                  | Type           | Value                   |
|----------------------|----------------|-------------------------|
| ▼ RememberedNetworks | Array          | (6 items)               |
| ▶ Item 0             | Diction...     | (11 items)              |
| ▶ Item 1             | Diction...     | (11 items)              |
| ▶ Item 2             | Diction...     | (11 items)              |
| ▶ Item 3             | Diction...     | (11 items)              |
| ▶ Item 4             | Diction...     | (11 items)              |
| ▼ Item 5             | Diction... + - | (11 items) ⬆            |
| AutoLogin            | Boolean        | NO                      |
| ▶ CachedScanRecord   | Diction...     | (13 items)              |
| Captive              | Boolean        | YES                     |
| Closed               | Boolean        | NO                      |
| Disabled             | Boolean        | NO                      |
| LastConnected        | Date           | Jun 12, 2012 1:07:23 PM |
| SSID                 | Data           | <50414e45 5241>         |
| SSIDString           | String         | PANERA                  |
| SecurityType         | String         | Open                    |
| SystemMode           | Boolean        | YES                     |
| TemporarilyDisabled  | Boolean        | NO                      |
| Version              | Number         | 10                      |

/Library/Preferences/SystemConfiguration/  
com.apple.network.identification.plist

| Key               | Type                 | Value                                                             |
|-------------------|----------------------|-------------------------------------------------------------------|
| ▼ Signatures      | Array                | (6 items)                                                         |
| ▶ Item 0          | Diction...           | (4 items)                                                         |
| ▼ Item 1          | Diction... (4 items) |                                                                   |
| Identifier        | String               | IPv4.Router=10.0.0.1;IPv4.RouterHardwareAddress=00:03:52:07:ec:8e |
| ▼ Services        | Array                | (1 item)                                                          |
| ▼ Item 0          | Diction...           | (3 items)                                                         |
| ▼ DNS             | Diction...           | (2 items)                                                         |
| DomainName        | String               | colubris.lan                                                      |
| ▼ ServerAddresses | Array                | (1 item)                                                          |
| Item 0            | String               | 10.0.0.1                                                          |
| ▼ IPv4            | Diction...           | (4 items)                                                         |
| ▼ Addresses       | Array                | (1 item)                                                          |
| Item 0            | String               | 10.0.0.179                                                        |
| InterfaceName     | String               | en1                                                               |
| Router            | String               | 10.0.0.1                                                          |
| ▼ SubnetMasks     | Array                | (1 item)                                                          |
| Item 0            | String               | 255.255.255.0                                                     |
| ServiceID         | String               | 7DCBE030-E96C-4A7E-86C5-9DD4ECA00B65                              |
| Signature         | String               | IPv4.Router=10.0.0.1;IPv4.RouterHardwareAddress=00:03:52:07:ec:8e |
| Timestamp         | Date                 | Jun 12, 2012 1:07:28 PM                                           |
| ▶ Item 2          | Diction...           | (4 items)                                                         |



# Determine “Home” Network

`com.apple.airport.preferences.plist`

- “Item 0”
- SecurityType != OPEN
  - “OPEN” generally seen at wifi hotspots
  - Example: My home network is “WPA2 Personal”

`system.log`

- More entries than most others when “airportd” searched for.

# Locational Data

# Wireless Networks

- Determine general location based upon SSID.
- com.apple.airport.preferences.plist
- Last Connected Time
  - Local System Time

| Key                 | Type       | Value                    |
|---------------------|------------|--------------------------|
| LastConnected       | Date       | Jun 13, 2012 9:16:56 AM  |
| SSID                | Data       | <76657972 6f6e>          |
| SSIDString          | String     | veyron                   |
| SecurityType        | String     | WPA2 Personal            |
| SystemMode          | Boolean    | YES                      |
| TemporarilyDisabled | Boolean    | NO                       |
| ▼ Item 1            | Diction... | (11 items)               |
| AutoLogin           | Boolean    | NO                       |
| ► CachedScanRecord  | Diction... | (14 items)               |
| Captive             | Boolean    | NO                       |
| Closed              | Boolean    | NO                       |
| Disabled            | Boolean    | NO                       |
| LastConnected       | Date       | Jun 2, 2012 7:28:21 AM   |
| SSID                | Data       | <57617368 696e6774 6f6e> |
| SSIDString          | String     | Washington Dulles WiFi   |
| SecurityType        | String     | Open                     |
| SystemMode          | Boolean    | YES                      |
| TemporarilyDisabled | Boolean    | NO                       |
| ▼ Item 2            | Diction... | (11 items)               |
| AutoLogin           | Boolean    | NO                       |
| ► CachedScanRecord  | Diction... | (15 items)               |
| Captive             | Boolean    | YES                      |
| Closed              | Boolean    | NO                       |
| Disabled            | Boolean    | NO                       |
| LastConnected       | Date       | Jun 6, 2012 1:33:59 PM   |
| SSID                | Data       | <4d617272 696f7474 2044> |
| SSIDString          | String     | Marriott Guest           |
| SecurityType        | String     | Open                     |
| SystemMode          | Boolean    | YES                      |
| TemporarilyDisabled | Boolean    | NO                       |
| ▼ Item 3            | Diction... | (11 items)               |
| AutoLogin           | Boolean    | NO                       |
| ► CachedScanRecord  | Diction... | (13 items)               |
| Captive             | Boolean    | YES                      |
| Closed              | Boolean    | NO                       |
| Disabled            | Boolean    | NO                       |
| LastConnected       | Date       | Jun 6, 2012 1:34:40 PM   |
| SSID                | Data       | <4d617272 696f7474 2044> |
| SSIDString          | String     | Marriott Conference      |
| SecurityType        | String     | Open                     |
| SystemMode          | Boolean    | YES                      |
| TemporarilyDisabled | Boolean    | NO                       |
| ▼ Item 4            | Diction... | (11 items)               |
| AutoLogin           | Boolean    | NO                       |
| ► CachedScanRecord  | Diction... | (14 items)               |
| Captive             | Boolean    | NO                       |
| Closed              | Boolean    | NO                       |
| Disabled            | Boolean    | NO                       |
| LastConnected       | Date       | Jun 6, 2012 5:40:22 PM   |
| SSID                | Data       | <434c544e 4554>          |
| SSIDString          | String     | CLTNET                   |

# Travel Timeline



# Detailed Timeline

## system.log- search “airportd”

```
Jun  1 19:52:04 bit airportd[3492]: _doAutoJoin: Already associated to “veyron”. Bailing on auto-join.
Jun  2 07:24:23 bit airportd[3848]: _doAutoJoin: Already associated to “Washington Dulles WiFi”. Bailing on
auto-join.
Jun  2 14:44:32 bit airportd[4944]: _doAutoJoin: Already associated to “Marriott Guest”. Bailing on auto-join.
Jun  3 17:12:14 bit airportd[6538]: _doAutoJoin: Already associated to “Marriott Guest”. Bailing on auto-join.
Jun  4 01:33:29 bit airportd[7841]: _doAutoJoin: Already associated to “Marriott Guest”. Bailing on auto-join.
Jun  5 08:50:16 bit airportd[17054]: _doAutoJoin: Already associated to “Marriott Guest”. Bailing on auto-
join.
Jun  6 13:34:01 bit airportd[20160]: _doAutoJoin: Already associated to “Marriott Guest”. Bailing on auto-
join.
Jun  6 13:34:40 bit airportd[20160]: _doAutoJoin: Already associated to “Marriott Conference”. Bailing on
auto-join.
Jun  6 17:40:23 bit airportd[20286]: _doAutoJoin: Already associated to “CLTNET”. Bailing on auto-join.
Jun  9 09:24:24 bit airportd[25724]: _doAutoJoin: Already associated to “veyron”. Bailing on auto-join.
Jun 12 13:07:24 bit airportd[3218]: _doAutoJoin: Already associated to “PANERA”. Bailing on auto-join.
Jun 12 16:49:03 bit airportd[3769]: _doAutoJoin: Already associated to “veyron”. Bailing on auto-join.
```

# Country Codes- kernel.log

## Search “country code”

```
Sep  1 17:42:13 MBP kernel[0]: en1: 802.11d country code set to 'AU'.
Sep  1 17:42:13 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44
48 52 56 60 64 149 153 157 161 165
Sep  1 17:46:13 MBP kernel[0]: Auth result for: 00:26:b0:fe:76:74 MAC AUTH succeeded
Sep  1 17:46:13 MBP kernel[0]: AirPort: Link Up on en1
...
Aug  5 09:49:07 MBP kernel[0]: en1: 802.11d country code set to 'X0'.
Aug  5 09:49:07 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 36 40 44 48 52
56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Aug  5 09:49:10 MBP kernel[0]: NVEthernet::setLinkStatus - Valid but not Active
Aug  5 09:49:10 MBP kernel[0]: NVEthernet::mediaChanged - Link is down
Aug  5 09:49:10 MBP kernel[0]: NVEthernet::setLinkStatus - Valid but not Active
Aug  5 09:49:13 MBP kernel[0]: en1: 802.11d country code set to 'US'.
Aug  5 09:49:13 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 36 40 44 48 52
56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Aug  5 09:49:40 MBP kernel[0]: Auth result for: 00:0c:e5:0e:65:bd MAC AUTH succeeded
Aug  5 09:49:40 MBP kernel[0]: AirPort: Link Up on en1
...
Jun  5 12:08:49 MBP kernel[0]: en1: 802.11d country code set to 'SE'.
Jun  5 12:08:49 MBP kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44
48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
Jun  5 12:09:14 MBP kernel[0]: Auth result for: 88:f0:77:2f:75:70 MAC AUTH succeeded
Jun  5 12:09:14 MBP kernel[0]: AirPort: Link Up on en1
```

# system.log

## Search Hostname" (10.6)

```
Apr 27 19:34:55 205-168-25-116 configd[13]: setting hostname to  
"205-168-25-116.dia.static.qwest.net"
```

- DIA – Denver Airport Code
- 205.168.25.116 – Registered to "JOHN Q HAMMONS HOTEL MANAGEMENT"

```
Aug 2 18:37:07 wsip-70-164-159-4 configd[13]: setting hostname  
to "wsip-70-164-159-4.lv.lv.cox.net"
```

- LV = Las Vegas?
- 70.164.159.4 – Registered to "Cox Communications Inc. NETBLK-LV-OHFC"

```
Jun 5 12:09:19 host-78-64-88-181 configd[13]: setting hostname  
to "host-78-64-88-181.homerun.telialia.com"
```

- 78.64.88.181 – Registered to Telia Network Services in Sweden

# Correlate with...

Photo  
EXIF Data

Calendar

Email  
Itineraries

Internet  
History

Travel  
Websites

Search  
History



# User Activity

# User Logins / Logouts

## Local Terminal

- May 28 14:48:04 byte login[693]: USER\_PROCESS: 693 ttys000
- May 28 14:48:07 byte login[698]: USER\_PROCESS: 698 ttys001
- May 28 15:07:29 byte login[812]: USER\_PROCESS: 812 ttys002
- May 28 15:07:51 byte login[812]: DEAD\_PROCESS: 812 ttys002

## Login Window

- May 28 12:42:23 byte loginwindow[66]: DEAD\_PROCESS: 74 console
- May 28 14:28:04 byte loginwindow[66]: USER\_PROCESS: 60 console

## SSH

- May 28 15:15:38 byte sshd[831]: USER\_PROCESS: 842 ttys002
- May 28 15:15:52 byte sshd[831]: DEAD\_PROCESS: 842 ttys002

## Screen Sharing

- 5/28/12 3:31:33.675 PM screensharingd: Authentication: SUCCEEDED ::  
User Name: Sarah Edwards :: Viewer Address: 192.168.1.101 :: Type:  
DH

# Log Analysis monthly.out

- Account Audit
- Monthly
- Uses `ac -p` command to calculate account time on system.
- “Accumulated connected time in decimal hours”

```
-- End of monthly output --  
  
Wed Apr  4 09:15:54 EDT 2012  
  
Rotating fax log files:  
  
Doing login accounting:  
      total      3678.85  
      sledwards  3678.76  
      root        0.09  
  
-- End of monthly output --  
  
Tue May  1 05:30:00 PDT 2012  
  
Rotating fax log files:  
  
Doing login accounting:  
      total      4301.95  
      sledwards  4301.77  
      root        0.18  
  
-- End of monthly output --  
  
Fri Jun  1 06:46:13 PDT 2012  
  
Rotating fax log files:  
  
Doing login accounting:  
      total      5047.22  
      sledwards  5047.04  
      root        0.18  
  
-- End of monthly output --
```

# Privilege Escalation

## SU

- 5/27/12 8:54:21.646 PM su: BAD SU oompa to root on /dev/ttys001
- 5/28/12 8:57:44.032 PM su: oompa to root on /dev/ttys000

## sudo

- 5/27/12 8:48:15.790 PM sudo: oompa :  
TTY=ttys000 ; PWD=/Users/oompa/Documents ;  
USER=root ; COMMAND=/usr/bin/iosnoop

# Account Creation

## Audit Logs

- ```
<record version="11" event="create user" modifier="0"
time="Mon May 28 21:25:49 2012" msec=" + 677 msec" >
<subject audit-uid="501" uid="501" gid="20" ruid="501"
rgid="20" pid="585" sid="100004" tid="585 0.0.0.0" />
<text>Create record type Users
&apos;supersecretuser&apos;; node &apos;;/Local/
Default&apos;;</text>
<return errval="success" retval="0" />
</record>
```

## secure.log

- ```
May 28 21:25:22 bit com.apple.SecurityServer[24]: UID
501 authenticated as user oompa (UID 501) for right
'system.preferences.accounts'
```

# Account Deletion

- /Library/Preferences/
  - com.apple.preferences.accounts.plist

| Key                         | Type       | Value                   |
|-----------------------------|------------|-------------------------|
| ▼ deletedUsers              | Array      | (2 items)               |
| ▶ Item 0                    | Diction... | (4 items)               |
| ▼ Item 1                    | Diction... | (4 items)               |
| dsAttrTypeStandard:RealName | String     | testuser                |
| dsAttrTypeStandard:UniqueID | Number     | 502                     |
| name                        | String     | testuser                |
| date                        | Date       | Jun 13, 2012 8:41:58 PM |

```
<record version="11" event="delete user" modifier="0" time="Wed Jun 13 20:41:56 2012"
msec=" + 322 msec" >
<subject audit-uid="501" uid="501" gid="20" ruid="501" rgid="20" pid="10717"
sid="100005" tid="10717 0.0.0.0" />
<text>Delete record type Users &apos;testuser&apos;; node &apos;;/Local/Default&apos;;</
text>
<return errval="success" retval="0" />
</record>
```

# Backups

# Backup Log Entry

## system.log

```
Jun 16 15:18:10 bit com.apple.backupd[1957]: Starting standard backup
Jun 16 15:18:10 bit com.apple.backupd[1957]: Attempting to mount network destination URL: afp://Sarah%20Edwards;AUTH=SRP@Delorean.local/Data
Jun 16 15:18:19 bit com.apple.backupd[1957]: Mounted network destination at mountpoint: /Volumes/Data using URL: afp://Sarah%20Edwards;AUTH=SRP@Delorean.local/Data
Jun 16 15:18:23 bit com.apple.backupd[1957]: QUICKCHECK ONLY; FILESYSTEM CLEAN
Jun 16 15:18:26 bit com.apple.backupd[1957]: Disk image /Volumes/Data/bit.sparsebundle mounted at: /Volumes/Time Machine Backups
Jun 16 15:18:26 bit com.apple.backupd[1957]: Backing up to: /Volumes/Time Machine Backups/Backups.backupdb
Jun 16 12:19:00 bit com.apple.backupd[1957]: 100.0 MB required (including padding), 516.13 GB available
Jun 16 12:19:00 bit com.apple.backupd[1957]: Waiting for index to be ready (101)
Jun 16 12:22:08 bit com.apple.backupd[1957]: Copied 1115 files (26.1 MB) from volume LION.
Jun 16 12:22:09 bit com.apple.backupd[1957]: 1.23 GB required (including padding), 516.13 GB available
Jun 16 12:22:51 bit com.apple.backupd[1957]: Copied 971 files (1.1 MB) from volume LION.
Jun 16 12:22:57 bit com.apple.backupd[1957]: Starting post-backup thinning
Jun 16 12:23:43 bit com.apple.backupd[1957]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/2012-05-19-004000 (21.3 MB)
Jun 16 12:24:22 bit com.apple.backupd[1957]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/2012-06-08-004822 (87.3 MB)
Jun 16 12:25:11 bit com.apple.backupd[1957]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/2012-06-10-002525 (168.2 MB)
Jun 16 12:25:11 bit com.apple.backupd[1957]: Post-back up thinning complete: 3 expired backups removed
Jun 16 12:25:11 bit com.apple.backupd[1957]: Backup completed successfully.
Jun 16 12:25:51 bit com.apple.backupd[1957]: Ejected Time Machine disk image.
Jun 16 12:25:51 bit com.apple.backupd[1957]: Ejected Time Machine network volume.
```



# Backups - /Library/Preferences/ com.apple.TimeMachine.plist

| Key                           | Type       | Value                                   |
|-------------------------------|------------|-----------------------------------------|
| ▶ FirmwareCheckDatesLion      | Diction... | (1 item)                                |
| ▶ HostUUIDs                   | Array      | (1 item)                                |
| LocalizedDiskImageVolumeName  | String     | Time Machine Backups                    |
| BackupAlias                   | Data       | <00000000 03e40002 00010444 61746100 00 |
| PreferencesVersion            | Number     | 1                                       |
| TimeCapsuleName               | String     | Delorean                                |
| RootVolumeUUID                | String     | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D    |
| FirmwareCheckDestinationAlias | Data       | <00000000 03e40002 00010444 61746100 00 |
| AutoBackup                    | Boolean    | YES                                     |
| ▶ DestinationVolumeUUIDs      | Array      | (1 item)                                |

\\Sarah Edwards\\afp://Sarah%20Edwards@Delorean.local/Data\\2afp://Sarah%20Edwards;AUTH=SRP@Delorean.local/Data

/var/db/  
com.apple.TimeMachine.SnapshotDates.plist

| Key                                    | Type  | Value                    |
|----------------------------------------|-------|--------------------------|
| ▼ 3F6992A5-4151-37CC-BD67-C6556DA81FB1 | Array | (60 items)               |
| Item 0                                 | Date  | Oct 2, 2011 8:36:25 PM   |
| Item 1                                 | Date  | Oct 15, 2011 11:34:12 AM |
| Item 2                                 | Date  | Oct 23, 2011 12:36:23 AM |
| Item 3                                 | Date  | Oct 30, 2011 12:21:28 AM |
| Item 4                                 | Date  | Nov 12, 2011 3:42:43 PM  |
| Item 5                                 | Date  | Nov 19, 2011 9:12:42 AM  |
| Item 6                                 | Date  | Nov 27, 2011 10:36:34 AM |
| Item 7                                 | Date  | Dec 4, 2011 8:43:46 AM   |
| Item 8                                 | Date  | Dec 11, 2011 9:12:43 AM  |
| Item 9                                 | Date  | Dec 18, 2011 10:27:37 AM |
| Item 10                                | Date  | Dec 28, 2011 7:47:02 PM  |
| Item 11                                | Date  | Jan 4, 2012 5:49:49 PM   |
| Item 12                                | Date  | Jan 11, 2012 7:05:02 PM  |
| Item 13                                | Date  | Jan 18, 2012 6:35:38 PM  |

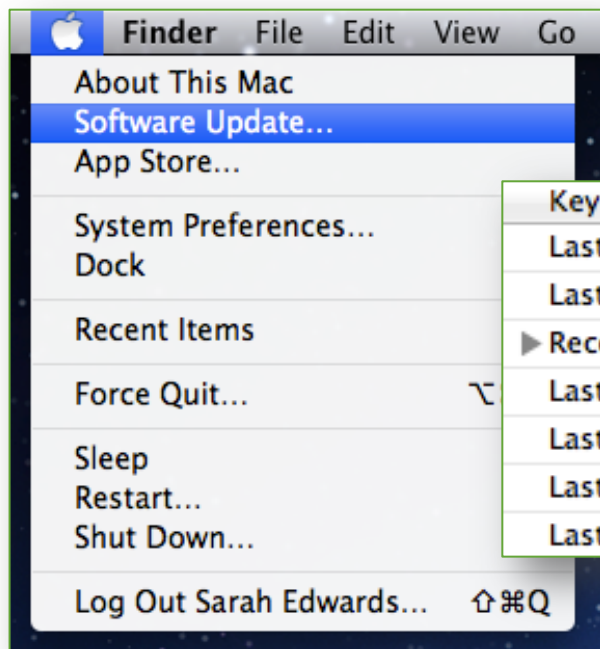
# Software

# Installed Software

## install.log – Search “Installed”

```
May  9 16:28:06 localhost OSInstaller[328]: Installed "Mac OS X" ()
...
May  9 19:56:21 bit installd[338]: Installed "Evernote" ()
May 10 00:45:34 bit installd[559]: Installed "Flashback malware removal tool" (1.0)
May 10 00:45:34 bit installd[559]: Installed "Mac OS X Update Combined" (10.7.4)
May 10 00:45:34 bit installd[559]: Installed "iTunes" (10.6.1)
May 10 00:46:33 bit installd[559]: Installed "Lion Recovery Update" (1.0)
May 10 16:51:51 bit installd[295]: Installed "Xcode" ()
May 10 16:55:55 bit installd[295]: Installed "iPhoto" ()
May 11 19:51:09 bit installd[4384]: Installed "Office 2011 14.1.0 Update" ()
May 14 18:31:44 bit installd[9572]: Installed "Java for OS X 2012-003" (1.0)
May 19 16:50:20 bit installd[20691]: Installed "TrueCrypt 7.1a" ()
May 19 17:17:25 bit installd[20847]: Installed "CCleaner" ()
May 19 17:32:19 bit installd[20847]: Installed "TextWrangler" ()
May 26 20:15:45 bit installd[39022]: Installed "The Unarchiver" ()
May 27 15:46:56 bit installd[41936]: Installed "Wireshark 1.6.8 Intel 64" ()
May 27 20:57:48 bit installd[514]: Installed "Microsoft Error Reporting for Mac" ()
May 27 20:59:41 bit installd[978]: Installed "Office 2011 14.2.2 Update" ()
```

/Library/Preferences/  
com.apple.SoftwareUpdate.plist



| Key                             | Type   | Value                   |
|---------------------------------|--------|-------------------------|
| LastAttemptSystemVersion        | String | 10.7.4 (11E53)          |
| LastRecommendedUpdatesAvailable | Number | 0                       |
| ▶ RecommendedUpdates            | Array  | (1 item)                |
| LastResultCode                  | Number | 100                     |
| LastUpdatesAvailable            | Number | 0                       |
| LastAttemptDate                 | Date   | Jun 19, 2012 9:58:37 AM |
| LastSuccessfulDate              | Date   | Jun 14, 2012 3:34:31 PM |

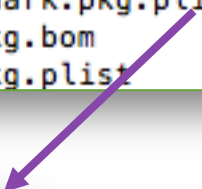
# /Library/Receipts/ InstallHistory.plist

| Key                  | Type       | Value                    |
|----------------------|------------|--------------------------|
| ▼ Item 27            | Diction... | (5 items)                |
| date                 | Date       | May 27, 2012 3:46:56 PM  |
| displayName          | String     | Wireshark 1.6.8 Intel 64 |
| displayVersion       | String     |                          |
| ▶ packageIdentifiers | Array      | (3 items)                |
| processName          | String     | Installer                |
| ▶ Item 28            | Diction... | (5 items)                |
| ▶ Item 29            | Diction... | (5 items)                |
| ▶ Item 30            | Diction... | (5 items)                |
| ▶ Item 31            | Diction... | (5 items)                |
| ▶ Item 32            | Diction... | (5 items)                |
| ▶ Item 33            | Diction... | (5 items)                |
| ▶ Item 34            | Diction... | (5 items)                |
| ▶ Item 35            | Diction... | (5 items)                |
| ▼ Item 36            | Diction... | (5 items)                |
| date                 | Date       | Jun 14, 2012 3:34:29 PM  |
| displayName          | String     | iTunes                   |
| displayVersion       | String     | 10.6.3                   |
| ▶ packageIdentifiers | Array      | (6 items)                |
| processName          | String     | Software Update          |

# Receipt Files

## /var/db/receipts/

```
-rw-r--r--  1 root  wheel  35290 May 27 15:46 org.wireshark.ChmodBPF.pkg.bom
-rw-r--r--  1 root  wheel    260 May 27 15:46 org.wireshark.ChmodBPF.pkg.plist
-rw-r--r--  1 root  wheel  62594 May 27 15:46 org.wireshark.Wireshark.pkg.bom
-rw-r--r--  1 root  wheel    256 May 27 15:46 org.wireshark.Wireshark.pkg.plist
-rw-r--r--  1 root  wheel  35138 May 27 15:46 org.wireshark.cli.pkg.bom
-rw-r--r--  1 root  wheel    255 May 27 15:46 org.wireshark.cli.pkg.plist
```



| Key                | Type   | Value                       |
|--------------------|--------|-----------------------------|
| PackageVersion     | String | 0.0.0.0                     |
| PackageIdentifier  | String | org.wireshark.Wireshark.pkg |
| InstallPrefixPath  | String | Applications                |
| InstallDate        | Date   | May 27, 2012 3:46:56 PM     |
| PackageFileName    | String | wireshark.pkg               |
| InstallProcessName | String | Installer                   |

# Install Details

## install.log

```
May 27 11:59:03 MBP Installer[470]: logKext Installation Log
May 27 11:59:03 MBP Installer[470]: Opened from: /Users/oomba/Downloads/
logKext-2.3.pkg
May 27 11:59:03 MBP Installer[470]: Product archive /Users/oomba/Downloads/
logKext-2.3.pkg trustLevel=100
May 27 11:59:17 MBP Installer[470]: InstallerStatusNotifications plugin loaded
May 27 11:59:26 MBP runner[477]: Administrator authorization granted.
May 27 11:59:26 MBP Installer[470]:
=====
May 27 11:59:26 MBP Installer[470]: User picked Standard Install
May 27 11:59:26 MBP Installer[470]: Choices selected for installation:
...
May 27 12:01:34 MBP installd[481]: Installed "logKext" ()
May 27 12:01:35 MBP installd[481]: PackageKit: ----- End install -----
```



# System Version

## install.log – Search “Build:”

**May 9 16:14:10 localhost Install Mac OS X Lion[339]: Running OS Build: Mac OS X 10.7 (11A511)**

May 9 16:19:25 localhost OSInstaller[328]: Running OS Build: Mac OS X 10.7 (11A511)

**May 11 19:23:47 bit Installer[3177]: Running OS Build: Mac OS X 10.7.4 (11E53)**

May 11 19:40:47 bit Installer[3755]: Running OS Build: Mac OS X 10.7.4 (11E53)

May 11 19:49:02 bit Installer[4114]: Running OS Build: Mac OS X 10.7.4 (11E53)

May 13 13:47:00 bit Installer[3927]: Running OS Build: Mac OS X 10.7.4 (11E53)

May 19 16:50:11 bit Installer[20680]: Running OS Build: Mac OS X 10.7.4 (11E53)

May 27 15:46:39 bit Installer[41929]: Running OS Build: Mac OS X 10.7.4 (11E53)

May 27 20:57:17 bit Installer[495]: Running OS Build: Mac OS X 10.7.4 (11E53)

May 27 20:58:01 bit Installer[529]: Running OS Build: Mac OS X 10.7.4 (11E53)

Jun 9 09:28:18 bit Installer[299]: Running OS Build: Mac OS X 10.7.4 (11E53)

# System Version

## kernel.log – Search “Darwin”

```
Jul 22 06:49:23 localhost kernel[0]: Darwin Kernel Version 11.0.0: Sat Jun 18 12:56:35 PDT
2011; root:xnu-1699.22.73~1/RELEASE_X86_64
...
Aug 8 21:43:11 localhost kernel[0]: Darwin Kernel Version 11.0.0: Sat Jun 18 12:56:35 PDT
2011; root:xnu-1699.22.73~1/RELEASE_X86_64
Aug 20 20:21:18 localhost kernel[0]: Darwin Kernel Version 11.1.0: Tue Jul 26 16:07:11 PDT
2011; root:xnu-1699.22.81~1/RELEASE_X86_64
...
Oct 5 06:59:00 localhost kernel[0]: Darwin Kernel Version 11.1.0: Tue Jul 26 16:07:11 PDT
2011; root:xnu-1699.22.81~1/RELEASE_X86_64
Oct 12 19:36:33 localhost kernel[0]: Darwin Kernel Version 11.2.0: Tue Aug 9 20:54:00 PDT
2011; root:xnu-1699.24.8~1/RELEASE_X86_64
...
Dec 30 19:21:03 localhost kernel[0]: Darwin Kernel Version 11.2.0: Tue Aug 9 20:54:00 PDT
2011; root:xnu-1699.24.8~1/RELEASE_X86_64
Feb 2 20:05:19 localhost kernel[0]: Darwin Kernel Version 11.3.0: Thu Jan 12 18:47:41 PST
2012; root:xnu-1699.24.23~1/RELEASE_X86_64
...
Apr 8 15:13:53 localhost kernel[0]: Darwin Kernel Version 11.3.0: Thu Jan 12 18:47:41 PST
2012; root:xnu-1699.24.23~1/RELEASE_X86_64
May 10 19:35:18 localhost kernel[0]: Darwin Kernel Version 11.4.0: Mon Apr 9 19:32:15 PDT
2012; root:xnu-1699.26.8~1/RELEASE_X86_64
```

# System Information & System State

# system.log

## Boot, Reboot & Shutdown

```
May 9 16:28:48 localhost bootlog[0]: BOOT_TIME 1336606128 0
May 10 16:40:27 localhost bootlog[0]: BOOT_TIME 1336682427 0
May 12 11:32:16 localhost bootlog[0]: BOOT_TIME 1336836736 0
May 27 20:02:41 localhost bootlog[0]: BOOT_TIME 1338163361 0
May 28 15:22:30 localhost bootlog[0]: BOOT_TIME 1338232950 0
Jun 9 09:27:05 localhost bootlog[0]: BOOT_TIME 1339248425 0
Jun 9 10:15:56 localhost bootlog[0]: BOOT_TIME 1339251356 0
Jun 9 10:33:39 localhost bootlog[0]: BOOT_TIME 1339252419 0
Jun 9 09:27:05 localhost bootlog[0]: BOOT_TIME 1339248425 0
Jun 9 10:15:56 localhost bootlog[0]: BOOT_TIME 1339251356 0
Jun 9 10:33:39 localhost bootlog[0]: BOOT_TIME 1339252419 0
Jun 10 13:33:56 localhost bootlog[0]: BOOT_TIME 1339349636 0
Jun 12 10:16:35 localhost bootlog[0]: BOOT_TIME 1339510595 0
```

```
May 27 20:02:14 bit shutdown[42801]: halt by oompa:
May 27 20:02:14 bit shutdown[42801]: SHUTDOWN_TIME: 1338163334 903688
May 28 15:20:06 bit shutdown[2421]: halt by oompa:
May 28 15:20:06 bit shutdown[2421]: SHUTDOWN_TIME: 1338232806 702175
Jun 9 09:25:33 bit shutdown[25868]: halt by oompa:
Jun 9 09:25:33 bit shutdown[25868]: SHUTDOWN_TIME: 1339248333 887656
Jun 9 10:15:24 bit shutdown[546]: reboot by oompa:
Jun 9 10:15:24 bit shutdown[546]: SHUTDOWN_TIME: 1339251324 30856
Jun 9 10:21:53 bit shutdown[309]: halt by oompa:
Jun 9 10:21:53 bit shutdown[309]: SHUTDOWN_TIME: 1339251713 535787
Jun 9 09:25:33 bit shutdown[25868]: halt by oompa:
Jun 9 09:25:33 bit shutdown[25868]: SHUTDOWN_TIME: 1339248333 887656
Jun 9 10:15:24 bit shutdown[546]: reboot by oompa:
Jun 9 10:15:24 bit shutdown[546]: SHUTDOWN_TIME: 1339251324 30856
Jun 9 10:21:53 bit shutdown[309]: halt by oompa:
Jun 9 10:21:53 bit shutdown[309]: SHUTDOWN_TIME: 1339251713 535787
```

# System Boot kernel.log

10.7

- Boot logging starts with  
“PMAP: PCID enabled”

10.6

- Boot logging starts with  
“npvhash=4095”



```
Jun 12 10:16:53 localhost kernel[0]: PMAP: PCID enabled
Jun 12 10:16:53 localhost kernel[0]: Darwin Kernel Version 11.4.0: Mon Apr  9 19:32:15 P
Jun 12 10:16:53 localhost kernel[0]: vm_page_bootstrap: 2011634 free pages and 69134 wi
Jun 12 10:16:53 localhost kernel[0]: kext submap [0xffffffff7f80732000 - 0xffffffff800000000
Jun 12 10:16:53 localhost kernel[0]: zone leak detection enabled
Jun 12 10:16:53 localhost kernel[0]: standard timeslicing quantum is 10000 us
Jun 12 10:16:53 localhost kernel[0]: mig_table_max_displ = 73
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=1 LocalApicId=0 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=2 LocalApicId=1 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=3 LocalApicId=4 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=4 LocalApicId=5 Enabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=5 LocalApicId=0 Disabled
Jun 12 10:16:53 localhost kernel[0]: AppleACPICPU: ProcessorId=6 LocalApicId=0 Disabled
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: npvhash=4095
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: PAE enabled
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: 64 bit mode enabled
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: Darwin Kernel Version 10.0.0: Fri Jul 31 22:47:34
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: vm_page_bootstrap: 1936010 free pages and 95606 w
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: standard timeslicing quantum is 10000 us
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: mig_table_max_displ = 73
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: AppleACPICPU: ProcessorId=0 LocalApicId=0 Enabled
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: AppleACPICPU: ProcessorId=1 LocalApicId=1 Enabled
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: calling mpo_policy_init for TMSafetyNet
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: Security policy loaded: Safety net for Time Machi
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: calling mpo_policy_init for Quarantine
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: Security policy loaded: Quarantine policy (Quaran
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: calling mpo_policy_init for Sandbox
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: Security policy loaded: Seatbelt sandbox policy (
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: Copyright (c) 1982, 1986, 1989, 1991, 1993
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: The Regents of the University of California. All
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: MAC Framework successfully initialized
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: using 16384 buffer headers and 4096 cluster IO bu
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: IOAPIC: Version 0x11 Vectors 64:87
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: ACPI: System State [S0 S3 S4 S5] (S3)
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: mbinit: done (64 MB memory set for mbuf pool)
Jun 12 10: Jun  5 12:07:52 localhost kernel[0]: rooting via boot-uuid from /chosen: 5D895F73-8DB0-
```



# System Boot Kernel & Processor Count

```
May  9 16:29:10 localhost kernel[0]: Darwin Kernel Version 11.0.0: Sat Jun 18 12:56:35 PDT 2011; root:xnu-1699.22.73~1/RELEASE_X86_64
```

```
...
```

```
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=1 LocalApicId=0 Enabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=2 LocalApicId=1 Enabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=3 LocalApicId=4 Enabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=4 LocalApicId=5 Enabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=5 LocalApicId=0 Disabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=6 LocalApicId=0 Disabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=7 LocalApicId=0 Disabled
May  9 16:29:10 localhost kernel[0]: AppleACPICPU: ProcessorId=8 LocalApicId=0 Disabled
```

# Hibernation Logging

## RAM Size

```
Jun  9 16:43:56 bit kernel[0]: hibernate image  
path: /var/vm/sleepimage  
Jun  9 16:43:58 bit kernel[0]: Opened file /  
var/vm/sleepimage, size 8589934592, partition  
base 0x0, maxio 400000 ssd 0
```



# System Boot

## Boot Device

```
May  9 16:29:10 localhost kernel[0]: rooting via boot-  
uuid from /chosen: 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D  
May  9 16:29:10 localhost kernel[0]: Waiting on <dict  
ID="0"><key>IOProviderClass</key><string  
ID="1">IOResources</string><key>IOResourceMatch</  
key><string ID="2">boot-uuid-media</string></dict>  
May  9 16:29:10 localhost kernel[0]: Got boot device =  
IOService:/AppleACPIPlatformExpert/PCI0@0/AppleACPIPCI/  
SATA@1F,2/AppleIntelPchSeriesAHCI/PRT0@0/IOAHCIDevice@0/  
AppleAHCIDiskDriver/IOAHCIBlockStorageDevice/  
IOBlockStorageDriver/WDC WD7500BPKT-75PK4T0 Media/  
IOGUIDPartitionScheme/Untitled@2
```

\_\_\_\_\_

|     |    |          |           |            |         |     |           |      |          |                                      |
|-----|----|----------|-----------|------------|---------|-----|-----------|------|----------|--------------------------------------|
| May | 9  | 16:29:10 | localhost | kernel[0]: | rooting | via | boot-uuid | from | /chosen: | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D |
| May | 10 | 16:40:56 | localhost | kernel[0]: | rooting | via | boot-uuid | from | /chosen: | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D |
| May | 12 | 11:32:30 | localhost | kernel[0]: | rooting | via | boot-uuid | from | /chosen: | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D |
| May | 27 | 20:03:02 | localhost | kernel[0]: | rooting | via | boot-uuid | from | /chosen: | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D |
| May | 28 | 15:22:40 | localhost | kernel[0]: | rooting | via | boot-uuid | from | /chosen: | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D |
| Jun | 9  | 09:27:16 | localhost | kernel[0]: | rooting | via | boot-uuid | from | /chosen: | 3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D |

```
bit:home oompa$ ioreg -p IODeviceTree -n chosen | more  
+--o Root <class IORegistryEntry, id 0x100000100, retain 10>  
  +--o / <class IOPlatformExpertDevice, id 0x100000110, registered, matched, active, busy 0 (17870 ms), retain 41>  
    +-o chosen <class IOService, id 0x100000101, !registered, !matched, active, busy 0, retain 5>  
      {  
        1 "boot-file-path" = <040450005c005300790073007...65006d005c004c006900620072006100720079005c0043006f0072005  
          "boot-kernelcache-adler32" = <760a732c>  
          "boot-args" = <&00>  
          "machine-signature" = <00000000>  
          "boot-uuid" = <"3981E2E6-0CAC-3A3E-BE1D-90D583F89A5D">  
          "efilogin-unlock-ident" = <"EDFD173B-778A-4191-8479-09F7E08B87AE">  
          "efilogin-user-ident" = <"EDFD173B-778A-4191-8479-09F7E08B87AE">  
          "bootroot-active" = <&>  
          "boot-file" = <"mach_kernel">  
          "name" = <"chosen">  
          "boot-device-path" = <02010c00d041030a0000000001010600021f03120a00000000000000004012a00030000000a8074157005  
      }  
}
```

# System Boot MAC Addresses

- Three different systems, boot from same HDD.
- Boot-UUID remains the same.
- MAC addresses change for each system.
- Correlate an HDD moving to/from systems.

```
Jun 14 17:41:59 localhost kernel[0]: rooting via boot-uuid from /chosen: 1FDCF218-B7EB-3BAC-9AD6-8498D0E2EA9D
Jun 14 19:50:26 localhost kernel[0]: rooting via boot-uuid from /chosen: 1FDCF218-B7EB-3BAC-9AD6-8498D0E2EA9D
Jun 14 20:33:38 localhost kernel[0]: rooting via boot-uuid from /chosen: 1FDCF218-B7EB-3BAC-9AD6-8498D0E2EA9D
```

```
Jun 14 17:42:22 Sarah-Edwardss-MacBook kernel[0]: yukon: Ethernet address 00:19:e3:3c:cb:7e
Jun 14 17:42:22 Sarah-Edwardss-MacBook kernel[0]: AirPort_AthrFusion21: Ethernet address 00:1b:63:c3:8d:1a
Jun 14 19:50:53 Sarah-Edwardss-MacBook kernel[0]: AirPort_Brcm4331: Ethernet address 28:cf:da:04:84:77
Jun 14 19:50:53 Sarah-Edwardss-MacBook kernel[0]: BCM5701Enet: Ethernet address 3c:07:54:03:65:20
Jun 14 20:34:12 Sarah-Edwardss-MacBook kernel[0]: BCM5701Enet: Ethernet address c4:2c:03:09:ca:fd
Jun 14 20:34:12 Sarah-Edwardss-MacBook kernel[0]: AirPort_Brcm43224: Ethernet address 90:27:e4:f8:e6:5f
```

# System Boot Shutdown Cause

Jul 23 17:08:52 localhost kernel[0]: Previous Shutdown Cause: #

0

- Battery Removal/Power Plug

3

- Hard Shutdown (Hold Power Button)

5

- Normal Shutdown/Reboot

-128

- Unknown

-60

- Unknown

# kernel.log

## Sleep Cause

May 26 17:27:02 MBP kernel[0]: Previous Sleep Cause: #

5

- Normal Sleep, Closed Laptop Lid

-60

- Unknown

0

- Hibernation

# kernel.log - Wake Reason

Jun 9 19:45:46 bit kernel[0]: Wake reason: <Message>

RTC (Alarm)

- Wake on Demand, Bonjour Services - Real Time Clock

EC LID0, EC LID0 EHC2

- Laptop Lid

EHC1, EHC2

- Enhanced Host Controller - USB, Bluetooth, Wireless Devices

PWRB (User)

- Power Button

OHC1

- Open Host Controller - USB/Firewire, Mouse/Keyboard

? (User)

- Power Button from hibernation w/ no battery power

USB1

- Trackpad

# Disk Usage History daily.log

Sun May 13 04:02:55 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

|            |       |       |       |     |   |
|------------|-------|-------|-------|-----|---|
| /dev/disk1 | 698Gi | 109Gi | 588Gi | 16% | / |
| /dev/disk1 | 698Gi | 123Gi | 574Gi | 18% | / |
| /dev/disk1 | 698Gi | 172Gi | 525Gi | 25% | / |
| /dev/disk1 | 698Gi | 181Gi | 517Gi | 26% | / |
| /dev/disk1 | 698Gi | 181Gi | 517Gi | 26% | / |
| /dev/disk1 | 698Gi | 180Gi | 517Gi | 26% | / |
| /dev/disk1 | 698Gi | 180Gi | 517Gi | 26% | / |

Disk status:

| Filesystem | Size  | Used  | Avail | Capacity | Mounted on |
|------------|-------|-------|-------|----------|------------|
| /dev/disk1 | 698Gi | 109Gi | 588Gi | 16%      | /          |

Network interface status:

| Name  | Mtu   | Network   | Address                 | Ipkts   | Ierrs | Opkts   | Oerrs | Coll |
|-------|-------|-----------|-------------------------|---------|-------|---------|-------|------|
| lo0   | 16384 | <Link#1>  |                         | 6641727 | 0     | 6641727 | 0     | 0    |
| lo0   | 16384 | localhost | fe80:1::1               | 6641727 | -     | 6641727 | -     | -    |
| lo0   | 16384 | 127       | localhost               | 6641727 | -     | 6641727 | -     | -    |
| lo0   | 16384 | localhost | ::1                     | 6641727 | -     | 6641727 | -     | -    |
| gif0* | 1280  | <Link#2>  |                         | 0       | 0     | 0       | 0     | 0    |
| stf0* | 1280  | <Link#3>  |                         | 0       | 0     | 0       | 0     | 0    |
| en0   | 1500  | <Link#4>  | c4:2c:03:09:ca:fd       | 0       | 0     | 0       | 0     | 0    |
| en1   | 1500  | <Link#5>  | 90:27:e4:f8:e6:5f       | 1823664 | 0     | 2065789 | 0     | 0    |
| p2p0* | 2304  | <Link#6>  | 02:27:e4:f8:e6:5f       | 0       | 0     | 0       | 0     | 0    |
| fw0   | 4078  | <Link#7>  | e8:06:88:ff:fe:d5:5d:08 | 0       | 0     | 0       | 0     | 0    |

Local system status:

4:03 up 16:31, 2 users, load averages: 10.59 2.96 1.20

# Printing



# /var/log/cups/page\_log

- Printer Name
- User
- Job ID
- Date/Time
- Page Number
- Copies
- Job Billing
- Originating Hostname
- Job Name
  - “Print - ..”
- Media
  - “Letter”
- Sides
  - “one-sided” or “-”

```
Brother_HL_2170W_series oompa 1 [31/May/2012:20:26:31 -0400] 1 1 - localhost Print - Amazon.com - Returns Center Letter -  
Brother_HL_2170W_series oompa 1 [31/May/2012:20:26:31 -0400] 2 1 - localhost Print - Amazon.com - Returns Center Letter -  
Brother_HL_2170W_series oompa 2 [31/May/2012:20:27:39 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided  
Brother_HL_2170W_series oompa 3 [01/Jun/2012:17:17:53 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided  
Brother_HL_2170W_series oompa 4 [01/Jun/2012:17:26:25 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided  
Brother_HL_2170W_series oompa 7 [01/Jun/2012:17:32:06 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided  
Brother_HL_2170W_series oompa 8 [01/Jun/2012:17:38:37 -0400] 1 1 - localhost Print - VIP.Zappos.com UPS Return Label Letter one-sided  
Brother_HL_2170W_series oompa 9 [14/Jun/2012:10:36:03 -0400] 1 1 - localhost Print - Platypus - Wikipedia, the free encyclopedia Letter -  
Brother_HL_2170W_series oompa 9 [14/Jun/2012:10:36:03 -0400] 2 1 - localhost Print - Platypus - Wikipedia, the free encyclopedia Letter -  
Brother_HL_2170W_series oompa 9 [14/Jun/2012:10:36:04 -0400] 3 1 - localhost Print - Platypus - Wikipedia, the free encyclopedia Letter -
```

# /var/log/cups/access\_log

- Hostname
- Group (-)
- User (-)
- Date/Time
- Method/Resource/  
Version
- Status Code
- 200 = Successful
- Bytes in Request
- IPP Operation
  - “Create-Job”
  - “Send Document”
- IPP Status
  - “successful-ok”

```
localhost - - [01/Jun/2012:17:32:00 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 1243 Create-Job successful-ok
localhost - - [01/Jun/2012:17:32:00 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 166037 Send-Document successful-ok
localhost - - [01/Jun/2012:17:32:01 -0400] "POST / HTTP/1.1" 200 345 Set-Job-Attributes successful-ok
localhost - - [01/Jun/2012:17:38:31 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 1243 Create-Job successful-ok
localhost - - [01/Jun/2012:17:38:31 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 166037 Send-Document successful-ok
localhost - - [01/Jun/2012:17:38:32 -0400] "POST / HTTP/1.1" 200 345 Set-Job-Attributes successful-ok
localhost - - [14/Jun/2012:10:35:57 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 1267 Create-Job successful-ok
localhost - - [14/Jun/2012:10:35:57 -0400] "POST /printers/Brother_HL_2170W_series HTTP/1.1" 200 570775 Send-Document successful-ok
localhost - - [14/Jun/2012:10:35:57 -0400] "POST / HTTP/1.1" 200 311 Set-Job-Attributes successful-ok
```

# Printer Control Files

## /private/var/spool/cups

- Nine Printer Control Jobs (c#####)

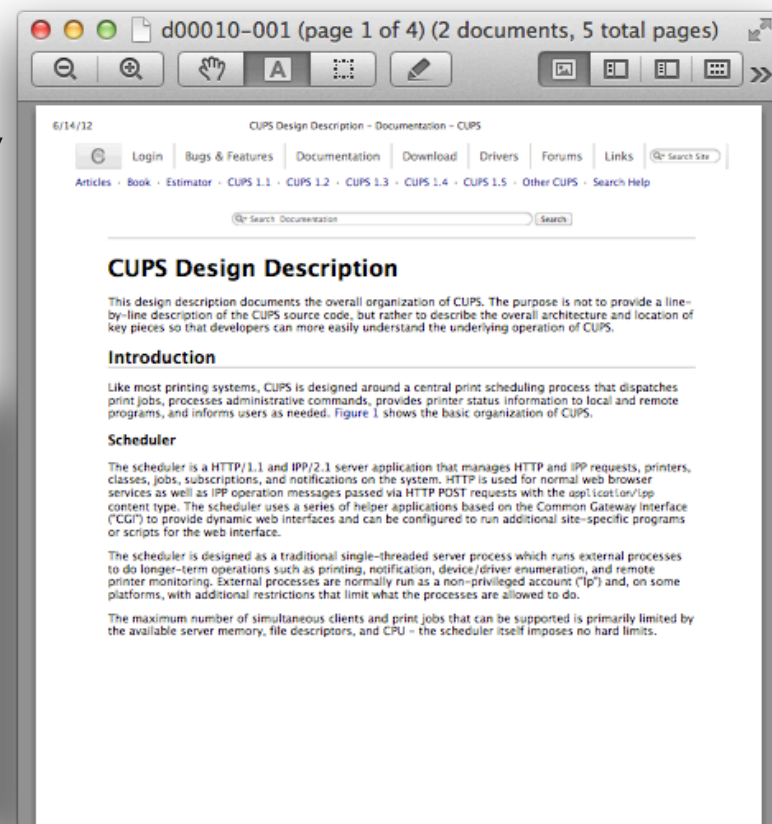
```
sh-3.2# pwd
/private/var/spool/cups
sh-3.2# ls -la
total 72
drwx--x--- 13 root  _lp      442 Jun 14 10:36 .
drwxr-xr-x  7 root  wheel    238 May  9 19:22 ..
-rw-----  1 root  _lp      1841 May 31 20:26 c00001
-rw-----  1 root  _lp      1883 May 31 20:27 c00002
-rw-----  1 root  _lp      1883 Jun  1 17:26 c00003
-rw-----  1 root  _lp      1883 Jun  1 17:31 c00004
-rw-----  1 root  _lp      1815 Jun  1 17:28 c00005
-rw-----  1 root  _lp       723 Jun  1 17:31 c00006
-rw-----  1 root  _lp      1883 Jun  1 17:33 c00007
-rw-----  1 root  _lp      1883 Jun  1 17:38 c00008
-rw-----  1 root  _lp      1873 Jun 14 10:36 c00009
drwxrwxr-x  8 root  _lp       272 Jun 14 10:46 cache
drwxrwx--T  2 root  _lp        68 Jun 19  2011 tmp
```

# Printer Data Files

## /private/var/spool/cups

- Data Files (d#####)?
- Removed immediately after successful print.
- PDF Files

```
drwx--x--- 15 root _lp      510 Jun 14 12:36 .
drwxr-xr-x  7 root wheel    238 May  9 19:22 ..
-rw-----  1 root _lp      1841 May 31 20:26 c00001
-rw-----  1 root _lp      1883 May 31 20:27 c00002
-rw-----  1 root _lp      1883 Jun  1 17:26 c00003
-rw-----  1 root _lp      1883 Jun  1 17:31 c00004
-rw-----  1 root _lp      1815 Jun  1 17:28 c00005
-rw-----  1 root _lp       723 Jun  1 17:31 c00006
-rw-----  1 root _lp      1883 Jun  1 17:33 c00007
-rw-----  1 root _lp      1883 Jun  1 17:38 c00008
-rw-----  1 root _lp      1873 Jun 14 10:36 c00009
-rw-----  1 root _lp      1878 Jun 14 12:36 c00010
drwxrwxr-x  8 root _lp       272 Jun 14 12:36 cache
-rw-r----- 1 root _lp    608373 Jun 14 12:35 d00010-001
drwxrwx--T  2 root _lp       68 Jun 19 2011 tmp
```



# Temporal Changes & Context

# Time Changes: Going Back in Time

```
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good  cachedValue:
1.000000
Jun 16 14:50:56: --- last message repeated 4 times ---
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 14:50:56 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good  cachedValue:
1.000000
Jun 16 14:50:56: --- last message repeated 1 time ---
Jun 16 14:50:56 bit System Preferences[1828]: **** ERROR: -[GEOCityPickerView _bindPublicToPrivateProperties]
UI is already bounded
Jun 16 14:50:59 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good  cachedValue:
1.000000
Jun 16 11:51:05: --- last message repeated 4 times ---
Jun 16 11:51:05 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 11:51:05 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good  cachedValue:
1.000000
Jun 16 11:51:06 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] Invalidating
_selectedCityLayer
Jun 16 11:51:06 bit System Preferences[1828]: -[GEOWorldTimeZoneView selectedCityLayer] all good  cachedValue:
1.000000
Jun 16 11:51:06 bit ntpd[1848]: proto: precision = 1.000 usec
```

# Time Changes: Time Zone - /etc/localtime

```
bit:etc oompa$ pwd
/etc
bit:etc oompa$ ls -l localtime
lrwxr-xr-x 1 root wheel 39 Jun 16 11:51 localtime
-> /usr/share/zoneinfo/America/Los_Angeles
```

# Time Changes: Back to the Future

```
_selectedCityLayer
Jun 16 12:08:04 bit System Preferences[1914]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 12:08:04: --- last message repeated 1 time ---
Jun 16 12:08:04 bit System Preferences[1914]: **** ERROR: -[GEOCityPickerView
_bindPublicToPrivateProperties] UI is already bounded
Jun 16 12:08:06 bit System Preferences[1914]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 15:08:09: --- last message repeated 9 times ---
Jun 16 15:08:09 bit System Preferences[1914]: WARNING: -[GEOTimezoneHitMap
fileNameAtLongitude:latitude:] no time zone area found
Jun 16 15:08:13 bit System Preferences[1914]: -[GEOWorldTimeZoneView selectedCityLayer] all good
cachedValue:1.000000
Jun 16 15:08:15: --- last message repeated 5 times ---
```



# Time Zone Changes

## daily.log – Search “2012”

Tue Jun 19 07:12:16 EDT 2012

Removing old temporary files:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Removing scratch fax files

Disk status:

| Filesystem                         | Size |
|------------------------------------|------|
| /dev/disk1                         | 698G |
| localhost:/7YF29FtTIvw--stDNEB0g6T | 698G |
| /dev/disk5s2                       | 1.8T |

Network interface status:

| Name  | Mtu   | Network   | Address         |
|-------|-------|-----------|-----------------|
| lo0   | 16384 | <Link#1>  |                 |
| lo0   | 16384 | localhost | fe80:1::1       |
| lo0   | 16384 | 127       | localhost       |
| lo0   | 16384 | localhost | ::1             |
| gif0* | 1280  | <Link#2>  |                 |
| stf0* | 1280  | <Link#3>  |                 |
| en0   | 1500  | <Link#4>  | c4:2c:03:09:ca: |
| en1   | 1500  | <Link#5>  | 90:27:e4:f8:e6: |
| en1   | 1500  | bit.local | fe80:5::9227:e4 |
| fw0   | 4078  | <Link#6>  | e8:06:88:ff:fe: |
| p2p0  | 2304  | <Link#7>  | 02:27:e4:f8:e6: |

Local system status:

7:12 up 4 days, 10:22, 5 users, load

-- End of daily output --

|         |    |          |     |      |
|---------|----|----------|-----|------|
| Tue Jun | 5  | 08:50:04 | EDT | 2012 |
| Wed Jun | 6  | 10:17:44 | EDT | 2012 |
| Thu Jun | 7  | 08:15:09 | EDT | 2012 |
| Fri Jun | 8  | 03:15:00 | EDT | 2012 |
| Sat Jun | 9  | 09:24:18 | EDT | 2012 |
| Sun Jun | 10 | 09:19:00 | EDT | 2012 |
| Mon Jun | 11 | 04:01:17 | EDT | 2012 |
| Tue Jun | 12 | 04:06:51 | EDT | 2012 |
| Wed Jun | 13 | 08:26:34 | EDT | 2012 |
| Thu Jun | 14 | 08:47:03 | EDT | 2012 |
| Fri Jun | 15 | 19:13:34 | EDT | 2012 |
| Sat Jun | 16 | 11:00:19 | EDT | 2012 |
| Sun Jun | 17 | 07:57:40 | PDT | 2012 |
| Mon Jun | 18 | 05:34:50 | PDT | 2012 |
| Tue Jun | 19 | 07:12:16 | EDT | 2012 |

# Temporal Context

- Carved & Extracted Files
- May not contain context
  - Year
  - Time Zone

```
Jun 19 07:13:14 bit kernel[0]: PPTP domain init
Jun 19 07:13:16 bit kernel[0]: nd6_setmtu: new link MTU on ppp0 (1276) is too small for IPv6
Jun 19 07:13:42 bit kernel[0]: IOSurface: buffer allocation size is zero
Jun 19 07:19:55 bit kernel[0]: hibernate image path: /var/vm/sleepimage
Jun 19 07:19:55 bit kernel[0]: sizeof(IOHibernateImageHeader) == 512
Jun 19 07:19:55 bit kernel[0]: Opened file /var/vm/sleepimage, size 8589934592, partition base 0x0, maxio 4000000 ssd 0
Jun 19 07:19:55 bit kernel[0]: hibernate image major 14, minor 0, blocksize 512, pollers 4
Jun 19 07:19:55 bit kernel[0]: hibernate_alloc_pages flags 00000000, gobbling 0 pages
Jun 19 07:19:55 bit kernel[0]: hibernate_setup(0) took 0 ms
Jun 19 07:19:55 bit kernel[0]: en1: BSSID changed to 00:19:07:96:03:10
Jun 19 07:19:55 bit kernel[0]: wlEvent: en1 en1 Link DOWN virtIf = 0
Jun 19 07:19:55 bit kernel[0]: AirPort: Link Down on en1. Reason 8 (Disassociated because station leaving).
```

# Date & Time Search

## Epoch & Other Formats

### kernel.log

- Jun 19 09:20:16 bit kernel[0]: nspace-handler-set-snapshot-time: **1340112018**
- Jun 12 10:08:15 bit kernel[0]: RTC: maintenance alarm **2012/6/12 14:08:14**, sleep **2012/6/12 12:08:46**

### system.log

- Jun 13 09:55:31 bit mtmd[64]: Set snapshot time: **1339595733** (current time: **1339595731**)
- Jun 12 10:16:35 localhost bootlog[0]: BOOT\_TIME **1339510595** 0
- Jun 9 10:21:53 bit shutdown[309]: SHUTDOWN\_TIME: **1339251713** 535787
- Jun 12 17:23:44 bit com.apple.backupd[4046]: Deleted /Volumes/Time Machine Backups/Backups.backupdb/bit/**2012-06-10-012553** (50.5 MB)
- Jun 12 10:17:42 bit [0x0-0x8008].com.google.Chrome[141]: **2012-06-12 14:17:42.785** Google Chrome Helper[196:207] Error received in message reply handler: Connection invalid

# Bluetooth

# Bluetooth Devices

## system.log – Search “blued”

```
Jun 17 09:36:26 bit com.apple.blued[3545]: link key found for device:  
70-cd-60-f6-eb-de  
Jun 17 09:36:26 bit com.apple.blued[3545]: link key found for device:  
e8-06-88-33-d9-e0  
Jun 17 12:57:00 bit blued[3853]: Removing Bluetooth configured device:  
00-24-ef-be-dc-07  
Jun 17 13:10:20 bit com.apple.blued[3853]: link key found for device:  
70-cd-60-f6-eb-de  
Jun 17 13:10:20 bit com.apple.blued[3853]: link key found for device:  
e8-06-88-33-d9-e0
```

# /Library/Preferences/ com.apple.Bluetooth.plist

| Key                            | Type       | Value             |
|--------------------------------|------------|-------------------|
| ▶ AudioHeadphones              | Array      | (1 item)          |
| ▶ DaemonNoRoleSwitchDeviceList | Array      | (1 item)          |
| BluetoothVersionNumber         | Number     | 3                 |
| ControllerPowerState           | Number     | 0                 |
| ▶ PANInterfaces                | Array      | (1 item)          |
| ▶ HIDDevices                   | Array      | (2 items)         |
| ▶ SCOAUDIODevices              | Diction... | (1 item)          |
| ▶ PersistentPorts              | Diction... | (2 items)         |
| ▼ DeviceCache                  | Diction... | (4 items)         |
| ▶ 00-24-ef-be-dc-07            | Diction... | (14 items)        |
| ▼ e8-06-88-33-d9-e0            | Diction... | (1 item)          |
| ClassOfDevice                  | Number     | 9536              |
| ▶ cc-6d-a0-2c-96-2e            | Diction... | (9 items)         |
| ▼ 70-cd-60-f6-eb-de            | Diction... | (1 item)          |
| ClassOfDevice                  | Number     | 9620              |
| ▶ PersistentPortsServices      | Diction... | (1 item)          |
| ▼ PairedDevices                | Array      | (3 items)         |
| Item 0                         | String     | 70-cd-60-f6-eb-de |
| Item 1                         | String     | 00-24-ef-be-dc-07 |
| Item 2                         | String     | e8-06-88-33-d9-e0 |

# Determine Bluetooth Class of Device

- /System/Library/Frameworks/  
IOBluetooth.framework/Headers/
  - Bluetooth.h
  - BluetoothAssignedNumbers.h

```
// Physical layout of the "class of device/service" field (see Bluetooth Assigned Numbers section 1.21)
//
// 2 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1
// 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0  <- Bit Transmission Order
//
// +-----+-----+-----+
// | octet 3 | octet 2 | octet 1 |  <- Octet Transmission Order
// +-----+-----+-----+
// <----- 11 bits -----> < 5 bits > <- 6 bits ->
//
// +-----+-----+-----+
// | Service Classes | Major Device Class | Minor Device Class | 0 0 |
// +-----+-----+-----+
// | | | | | | | | | | * | * | * | | | | |
//
// +-----+-----+-----+
// | | | | | | | | | | + Limited Discoverable + Format Type
//
// | | | | | | | | | | + Networking //
// | | | | | | | | | | + Rendering // Device Class Major
// | | | | | | | | | | + Capturing //
// | | | | | | | | | | + Object Transfer //
// | | | | | | | | | | + Audio
// | | | | | | | | | | + Telephony enum
// | | | | | | | | | | + Information {
```

```
enum
{
    kBluetoothDeviceClassMajorMiscellaneous
    kBluetoothDeviceClassMajorComputer
    kBluetoothDeviceClassMajorPhone
    kBluetoothDeviceClassMajorLANAccessPoint
    kBluetoothDeviceClassMajorAudio
    kBluetoothDeviceClassMajorPeripheral
    kBluetoothDeviceClassMajorImaging
    kBluetoothDeviceClassMajorWearable
    kBluetoothDeviceClassMajorToy
    kBluetoothDeviceClassMajorHealth
    kBluetoothDeviceClassMajorUnclassified
}
```

Calculator

9536

ASCII Unicode Hide Binary 8 10 16

0000 0000 0000 0000 0000 0000 0000 0000

63 47 37

0000 0000 0000 0000 0010 0101 0100 0000

31 15 0

= 0x00, // [00000] Miscellaneous  
 = 0x01, // [00001] Desktop, Notebook, PDA, Organizers, etc...  
 = 0x02, // [00010] Cellular, Cordless, Payphone, Modem, etc...  
 = 0x03, // [00011] LAN Access Point  
 = 0x04, // [00100] Headset, Speaker, Stereo, etc...  
 = 0x05, // [00101] Mouse, Joystick, Keyboards, etc...  
 = 0x06, // [00110] Printing, scanner, camera, display, etc...  
 = 0x07, // [00111] Wearable  
 = 0x08, // [01000] Toy  
 = 0x09, // [01001] Health devices  
 = 0x1F, // [11111] Specific device code not assigned

# Log2Timeline

- Current Capabilities
  - macosx.lst
    - Generic Linux
    - FireFox
    - Syslog
    - Quarantine
    - Safari
    - Apache
    - etc.
- Future Work
  - Always more potential modules.
  - I need to re-learn perl.





# Analysis & Correlation of Mac Logs

Sarah Edwards

@iamevltwin

oompa@csh.rit.edu

---